

In the claims:

This listing of claims will replace all prior versions and listings of claims in the application:

- 1 1. (canceled).
- 1 2. (previously presented) The method of claim 31, including using said associated session key in response to another request to initiate a communication session from a third station received by the first station during said particular session key initiation interval, and using other session keys from the set of ephemeral session keys after expiry of said particular session key initiation interval.
- 1 3. (previously presented) The method of claim 2, including associating a unique set of intermediate data keys with each session key.
- 1 4. (previously presented) The method of claim 31, including:
  - 2 providing a buffer at the first station;
  - 3 storing the set of ephemeral session keys in the buffer; and
  - 4 removing session keys from said buffer upon expiry of respective session key lifetimes, said session key lifetimes being longer than the respective session key initiation intervals.
- 1 5. (canceled).
- 1 6. (previously presented) The method of claim 4, wherein the session key lifetimes have respective lengths longer or equal to a time required for verification of mutual authentication using said first and second sets of exchanges in expected circumstances.
- 1 7. (previously presented) The method of claim 4, wherein the session key lifetimes have respective lengths which are a multiple M times a time required for verification of mutual authentication using said first and second sets of exchanges in expected circumstances, where M is less than or equal to 10.

1 8. (canceled).

1 9. (previously presented) The apparatus of claim 34, including logic to use said associated  
2 session key in response to another request to initiate a communication session from a third  
3 station received by the first station during said particular session key initiation interval, and using  
4 other session keys from the set of ephemeral session keys after expiry of said particular session  
5 key initiation interval.

1 10. (previously presented) The apparatus of claim 9, including logic to associate a unique set of  
2 intermediate data keys with each session key.

1 11. (previously presented) The apparatus of claim 34, including  
2 a buffer at the first station;  
3 logic to store the set of ephemeral session keys in the buffer and to remove session keys  
4 in said set of ephemeral session keys from said buffer after expiry of the respective session key  
5 lifetimes, said session key lifetimes being longer than the respective session key initiation  
6 intervals.

1 12. (canceled).

1 13. (previously presented) The apparatus of claim 11, wherein the session key lifetimes have  
2 respective lengths longer or equal to a time required for verification of mutual authentication  
3 using said first and second sets of exchanges.

1 14. (previously presented) The apparatus of claim 11, wherein the session key lifetimes have  
2 respective lengths which are a multiple M times a time required for verification of mutual  
3 authentication using said first and second sets of exchanges in expected circumstances.

1 15-30. (canceled).

1 31. (previously presented) A method for mutual authentication in communications between first  
2 and second stations, comprising:

3 generating and storing a set of ephemeral session keys at the first station, ephemeral  
4 session keys in the set being associated with respective session key initiation intervals, and being  
5 discarded at a time later than expiration of the respective session key initiation intervals;

6 in response to a request to initiate a communication session received by the first station  
7 during a particular session key initiation interval, selecting the associated session key;

8 sending a message carrying said associated session key to the second station, and  
9 receiving a response from the second station including a digital identifier, the digital identifier  
10 being information shared between the first station and the second station, or between the first  
11 station and a user at the second station, the digital identifier being encrypted using said  
12 associated session key to verify receipt of the session key by the second station and to identify  
13 the second station or the user of the second station;

14 generating and storing, in the first station, a set of intermediate data keys, the set of  
15 intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being  
16 discarded at a time later than expiration of the particular session key initiation interval;

17 executing a first set of exchanges including one or more exchanges with the second  
18 station, after verifying in said first station receipt of the session key by the second station by  
19 decrypting the digital identifier using the associated session key at the first station and positively  
20 matching the decrypted digital identifier against an existing entry in a stored list of authorized  
21 users, the first set of exchanges including

22 sending a message to the second station carrying intermediate data key (i) from said  
23 set of intermediate data keys encrypted using the associated session key for a  
24 first exchange in first set of exchanges and using the intermediate data key (i-  
25 1) for subsequent exchanges in the first set of exchanges,

26 receiving a response from the second station including a hashed version of  
27 intermediate data key (i) encrypted using intermediate data key (i), decrypting  
28 the hashed version of the intermediate data key (i), calculating a hashed  
29 version of intermediate data key (i) at the first station, and matching the  
30 calculated hashed version and the received hashed version of intermediate data  
31 key (i) to verify receipt by the second station of intermediate data key (i);

32                   executing a second set of exchanges for mutual authentication after verifying in said first  
33 station receipt of the intermediate data key (n-1) by the second station, including  
34                   sending a first message carrying intermediate data key (n) encrypted using a hashed  
35                   version of a first shared secret,  
36                   receiving a response from the second station carrying a hashed version of intermediate  
37                   data key (n) encrypted using a hashed version of the first shared secret, and  
38                   decrypting the hashed version of the intermediate data key (n) , calculating a  
39                   hashed version of intermediate data key (n) at the first station, and matching  
40                   the calculated hashed version and the decrypted hashed version of intermediate  
41                   data key (n) to verify possession by the second station of the first shared  
42                   secret;  
43                   sending a second message carrying intermediate data key (n) encrypted using a hashed  
44                   version of a second shared secret; and  
45                   if the second station sends a response to the second message, carrying a hashed  
46                   version of intermediate data key (n) encrypted using a hashed version of the  
47                   second shared secret, after possession by the first station of the second shared  
48                   secret is verified at the second station, the verifying being accomplished at the  
49                   second station by decrypting the intermediate data key (n) from the second  
50                   message using the hashed version of the second shared secret, calculating a  
51                   hashed version of the intermediate data key (n), and matching the calculated  
52                   hashed version and the decrypted hashed version of intermediate data key (n)  
53                   to verify possession by the first station of the second shared secret, then  
54                   receiving the response from the second station, and decrypting the hashed version of  
55                   the intermediate data key (n) using the hashed version of the second shared  
56                   secret, calculating a hashed version of intermediate data key (n) at the first  
57                   station, and matching the calculated hashed version and the decrypted hashed  
58                   version of intermediate data key (n) at the first station to verify mutual  
59                   authentication of the first and second stations; and  
60                   if mutual authentication is verified at the first station, then sending a message indicating  
61                   successful authentication.

1 32. (previously presented) The method of claim 31, wherein said message indicating successful  
2 authentication carries a signal encrypted using intermediate data key (n-1) or using another  
3 prearranged one of said intermediate data keys (i).

1 33. (previously presented) The method of claim 31, including using intermediate data key (n) as  
2 a symmetrical key to encrypt data during post-authentication in-communications between the  
3 first and second stations in the communication session.

1 34.(previously presented) A data processing apparatus, comprising:

2 a processor associated with a first station, a communication interface adapted for  
3 connection to a communication medium, and memory storing instructions for execution by the  
4 data processor, the instructions including

5 logic to receive a request via the communication interface for initiation of a  
6 communication session between a first station and a second station;

7 logic to provide for mutual authentication in communications between the first station  
8 and a second station, comprising:

9 generating and storing a set of ephemeral session keys at the first station, ephemeral  
10 session keys in the set being associated with respective session key initiation intervals, and being  
11 discarded at a time later than expiration of the respective session key initiation intervals;

12 in response to a request to initiate a communication session received by the first station  
13 during a particular session key initiation interval, selecting the associated session key;

14 sending a message carrying said associated session key to the second station, and  
15 receiving a response from the second station including a digital identifier, the digital identifier  
16 being information shared between the first station and the second station, or between the first  
17 station and a user at the second station, the digital identifier being encrypted using said  
18 associated session key to verify receipt of the session key by the second station and to identify  
19 the second station or the user of the second station;

20 generating and storing, in the first station, a set of intermediate data keys, the set of  
21 intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being  
22 discarded at a time later than expiration of the particular session key initiation interval;

23 executing a first set of exchanges including one or more exchanges with the second

24 station, after verifying in said first station receipt of the session key by the second station by  
25 decrypting the digital identifier using the associated session key at the first station and positively  
26 matching the decrypted digital identifier against an existing entry in a stored list of authorized  
27 users, the first set of exchanges including

28 sending a message to the second station carrying intermediate data key (i) from said  
29 set of intermediate data keys encrypted using the associated session key for a  
30 first exchange in first set of exchanges and using the intermediate data key (i-  
31 1) for subsequent exchanges in the first set of exchanges,

32 receiving a response from the second station including a hashed version of  
33 intermediate data key (i) encrypted using intermediate data key (i), ~~and~~  
34 decrypting the hashed version of the intermediate data key (i), calculating a  
35 hashed version of intermediate data key (i) at the first station, and matching the  
36 calculated hashed version and the received hashed version of intermediate data  
37 key (i) to verify receipt by the second station of intermediate data key (i);

38 executing a second set of exchanges for mutual authentication after verifying in said first  
39 station receipt of the intermediate data key (n-1) by the second station, including

40 sending a first message carrying intermediate data key (n) encrypted using a hashed  
41 version of a first shared secret,

42 receiving a response from the second station carrying a hashed version of intermediate  
43 data key (n) encrypted using a hashed version of the first shared secret, and  
44 decrypting the hashed version of the intermediate data key (n) , calculating a  
45 hashed version of intermediate data key (n) at the first station, and matching  
46 the calculated hashed version and the decrypted hashed version of intermediate  
47 data key (n) to verify possession by the second station of the first shared  
48 secret;

49 sending a second message carrying intermediate data key (n) encrypted using a hashed  
50 version of a second shared secret; and

51 if the second station sends a response to the second message, carrying a hashed  
52 version of intermediate data key (n) encrypted using a hashed version of the  
53 second shared secret, after possession by the first station of the second shared  
54 secret is verified at the second station, the verifying being accomplished at the

55 second station by decrypting the intermediate data key (n) from the second  
56 message using the hashed version of the second shared secret, calculating a  
57 hashed version of the intermediate data key (n), and matching the calculated  
58 hashed version and the decrypted hashed version of intermediate data key (n)  
59 to verify possession by the first station of the second shared secret, then  
60 receiving the response from the second station, and decrypting the hashed version of  
61 the intermediate data key (n) using the hashed version of the second shared  
62 secret, calculating a hashed version of intermediate data key (n) at the first  
63 station, and matching the calculated hashed version and the decrypted hashed  
64 version of intermediate data key (n) at the first station to verify mutual  
65 authentication of the first and second stations; and  
66 if mutual authentication is verified at the first station, then sending a message indicating  
67 successful authentication.

1 35. (previously presented) The apparatus of claim 34, wherein said message indicating successful  
2 authentication carries a signal encrypted using intermediate data key (n-1) or using another  
3 prearranged one of said intermediate data keys (i).

1 36. (previously presented) The apparatus of claim 34, including using intermediate data key (n)  
2 as a symmetrical key to encrypt data during post-authentication communications between the  
3 first and second stations in the communication session.

1 37-39. (canceled).

///